Cisco ASA Express Security (500-260)

Exam Description: The Cisco ASA Express Security (SAEXS) exam is a 60 minute, 45 – 55 question assessment that assesses the candidate on the skills required to understand how the ASA functions, including FirePOWER services for ASA, while focusing on how to deploy and manage the Cisco ASA. This exam is required for partners to attain ASA Express Security Specialization.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

25% 1.0 ASA Product Overview: Platform and Positioning

1.1 Give a high-level overview of Cisco ASA NGFW solution, platform, and security services
1.2 Describe management tools
1.3 Describe base features
1.4 Describe license features
1.5 Describe platform and performance
1.6 Describe where Cisco ASA platforms are placed in the network

1.7 Configure basic connectivity
 1.7.a Managing boot process
 1.7.b Managing Cisco ASA with ASDM
 1.7.c Basic Cisco ASDM features
 1.7.d Basic upgrade
 1.7.e Interface security level
 1.7.f Configure static route, DHCP, NTP
 1.7.g Configure VLANs

1.8 Implement routing
 1.8.a Configure static routing
 1.8.b Configure dynamic routing

1.9 Configure backup and restore

1.10 Configure basic access control foundation
 1.10.a Configure interface ACL
 1.10.b Configure global ACL
 1.10.c Configure object groups
 1.10.d Implement NAT

1.11 Describe active/standby HA

35% 2.0 ASA FirePOWER Services: Positioning and Best Practices

2.1 Positioning, platforms, licensing, and services

2.2 Management considerations

2.2.a Cisco FireSIGHT Management Center

2.2.b Cisco Adaptive Security Device Manager

2.2.c Cisco Security Manager

2.2.d SFR module management interfaces

2.3 SFR initialization and traffic redirection

2.4 FireSIGHT policies and system basics

2.4.a Policy types

2.4.b Security zones

2.4.c Active directory integration

2.4.d Network discovery

2.5 Implement intrusion policy

2.6 Implement access policies

2.7 Implement file policies

2.8 Implement user context

2.9 Implement system and health policies

2.10 Event and system monitoring

2.10.a Impact levels

2.10.b Indications of compromise

2.10.c Event types

2.10.d Monitoring and dashboards

25% 3.0 ASA VPN Features, Positioning and Best Practices

3.1 Introduction

3.2 Describe management of Cisco ASA VPN

3.3 Describe remote access VPN

3.3.a Cisco AnyConnect Mobile Security Client

3.3.b Cisco AnyConnect Mobile Security Client: Network Access Manager

3.3.c Configure full-tunnel SSL VPN

3.3.d Configure Web VPN

3.3.e Configure XML profiles

3.3.f OS integration options

3.3.g Customize user interface

3.4 Describe site-to-site VPN

10% 4.0 ASA Licensing

- 4.1 Introduction

- 4.2 Describe feature licensing
  - 4.2.a Security plus
  - 4.2.b Web security essentials
  - 4.2.c Cloud web security
  - 4.2.d Botnet filtering
  - 4.2.e Cisco AnyConnect mobile security premium and essentials
  - 4.2.f Security context

- 4.3 Describe license changes
  - 4.3.a Permanent
  - 4.3.b Time-based
  - 4.3.c Share Cisco AnyConnect

- 4.4 Describe license management

5% 5.0 ASA Cloud Web Security

- 5.1 Implement cloud web security
  - 5.1.a Configure CWS proxy on Cisco ASA
  - 5.1.b Cisco ScanCenter integration

- 5.2 AMP and CTA